

Form PTO 1449

U.S. Department of Commerce  
Patent and Trademark Office

Information Disclosure Statement by Applicant

ATTY. DOCKET NUMBER  
NITT.0028

APPLICANT  
KAMINAGA et al

FILING DATE  
Concurrently Herewith

CLASS NUMBER 09/9356  
To Be Assigned 54

GROUP  
2124

U.S. PTO  
09/985654  
08/24/01

### U.S. Patent Documents

Examiner Initial	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB- CLASS	FILING DATE

### Foreign Patent Documents

Examiner Initial	DOCUMENT NUMBER	FILING DATE	COUNTRY	CLAS S	SUB- CLASS	TRANSLATION	
						Yes	No

### Other Documents (Including Author, Title, Date Pertinent Pages, Etc.)

		<del>Smart Card Handbook, pp. 263</del>
CD		Ross Anderson and Markus Kuhn, "Tamper Resistance -- A Cautionary Note", The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, Nov. 18-21, 1996, pp. 1-11
CP		Marc Joye, Arjen K. Lenstra and Jean-Jacques Quisquater, "Chinese Remaindering Based Cryptosystems in the Presence of Faults", to appear in Journal of Cryptology, pp. 1-5
CP		Peter Montgomery, "Modular Multiplication Without Trial Division", Mathematics of Computation, Volume 44, No. 170, April 1985, pp. 519-521.

EXAMINER

*[Signature]*

DATE CONSIDERED

7/5/04

EXAMINER: Initial if citation is considered, whether or not citation is in conformance with MPEP 609; draw a line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant

PTO1449

BEST AVAILABLE COPY

Form PTO 1449

U.S. Department of Commerce  
Patent and Trademark Office

Information Disclosure Statement by Applicant

ATTY. DOCKET NUMBER  
Nitt-0028

SERIAL NUMBER  
To be assigned  
09/93654

APPLICANT  
KAMINAGA et al.

FILING DATE  
Concurrently herewith

GROUP  
2184

RECEIVED  
JAN 14 2002  
Technology Center 2100

TRADEMARK OFFICE

U.S. Patent Documents

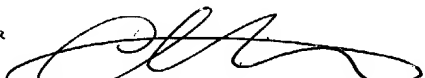
Examiner Initial	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE

Foreign Patent Documents

Examiner Initial	DOCUMENT NUMBER	FILING DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
						YES	NO
CD	EP 0 801 345 A1	4/2/97	EPO			X	
CD	EP 1 006 492 A1	11/25/99	EPO			X	
CD	EP 1 134 653 A2	3/15/01	EPO			X	

Other Documents (Including Author, Title, Date Pertinent Pages, Etc.)

CD	Paul C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems, Advances in Cryptology - Crypto 96, 16 <sup>th</sup> Annual International Cryptology Conference, Aug 18-22, 1996, Vol. Conf. 16, pp. 104-113.
CD	Thomas S. Messerges, Ezzy A. Dabbish, Robert H. Sloan, "Power Analysis Attacks of Modular Exponentiation on Smartcards", Cryptographic Hardware and Embedded Systems, International workshop August 1999, pp 144-157

EXAMINER 

DATE CONSIDERED 7/5/04

EXAMINER: Initial if citation is considered, whether or not citation is in conformance with MPEP 609; draw a line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant

PTO1449

BEST AVAILABLE COPY